USAWC STRATEGY RESEARCH PROJECT

A FLIGHT PLAN TOWARD A DEPARTMENT OF DEFENSE STRATEGY TO OPERATIONALIZE AND INTEGRATE GLOBAL NETWORK OPERATIONS (NETOPS)

by

Lieutenant Colonel John M. Odey
United States Air Force

Colonel David J. Smith
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **15 MAR 2006**	2. REPORT TYPE	3. DATES COVERED **00-00-2005 to 00-00-2006**
4. TITLE AND SUBTITLE **Flight Plan Toward a Department of Defense Strategy to Operationalize and Integrate Global Network Operations (NetOps)**		5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **John Odey**		5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**32**	

ABSTRACT

AUTHOR: Lieutenant Colonel John M. Odey

TITLE: A Flight Plan Toward a Department of Defense Strategy to Operationalize and Integrate Global Network Operations (NetOps)

FORMAT: Strategy Research Project

DATE: 10 March 2006 WORD COUNT: 7269 PAGES: 32

KEY TERMS: Communications, C4, Information, Global Information Grid (GIG)

CLASSIFICATION: Unclassified

Assured, timely, and relevant information is critical to effective warfighting. Global Network Operations (NetOps) provides the construct to provide this information to the right person at the right time, ideally in the right context. A DoD strategy to operationalize and integrate Global NetOps is necessary to set the proper direction and assimilate warfighting information ends, ways, and means. NetOps strategy must include well defined roles and responsibilities for all major elements, a single, effective command and control structure with proper governance, required resources, common understanding among all services and agencies, and integration into the full spectrum of DoD operations. The NetOps strategy should nest directly within national-level strategies, including the National Military Strategy and National Strategy to Secure Cyberspace. In addition, DoD must take action to develop a common set of NetOps goals and objectives, manage NetOps as an operational weapons system, provide the Commander, U.S. Strategic Command authority and responsibility over all DoD NetOps funding and programs, and establish a directing NetOps Council with flag officer representation from all combatant commands, services, and defense agencies. The end result is a construct to enable transformational joint operations concepts, facilitate network centric operations, and ensure DoD continues to optimize warfighting capabilities.

A FLIGHT PLAN TOWARD A DEPARTMENT OF DEFENSE STRATEGY TO OPERATIONALIZE AND INTEGRATE GLOBAL NETWORK OPERATIONS (NETOPS)

The vital importance of information to warfighting is certainly not new, but cannot be taken for granted. Emphasizing the importance of information, the National Defense Strategy states "successful military operations depend on the ability to protect information infrastructure and data… [and] bringing decisive capabilities to bear increasingly will rely on our capacity to harness and protect advantages in the realm of information."[1] Global Network Operations (NetOps) is the construct that ensures the provision of the right information at the right time to the right people, and is essential to Department of Defense (DoD) command and control. This means effective NetOps is indispensable to optimize the chances of winning the nation's wars and conflicts. Unfortunately NetOps across the DoD remains a relatively esoteric concept. Most in DoD consider the concept as just being within the realm of the technical experts from each of the military services and the Defense Information Systems Agency (DISA), among others, and not the operational warfighters. Further, most expect that NetOps is just automatically "there" providing information services. However, without NetOps, information is not managed, sent, delivered, stored, nor secured. This misperception also limits warfighters' ability to navigate within the sea of information, and prevents far ranging transformation to truly joint network centric operations. DoD must take positive action to guarantee information flow, and must establish NetOps as "operations," and integrate it across the spectrum of warfighting capabilities and functions. This drives the need for an overall DoD NetOps strategy to set proper direction and assimilate warfighting information ends, ways, and means. The NetOps strategy must include well defined roles and responsibilities for all major elements, a single, effective command and control structure with proper governance, required resources, a common understanding among all services and DoD organizations, and integration across the continuum of DoD operations. DoD must take action now to stay ahead of the technology power curve, and continue to optimize warfighting capabilities.

To obtain this warfighting edge, this paper will address the path toward an operational and integrated DoD NetOps strategy. Beginning with background information on NetOps, including a definition, a brief discussion of each of the elements comprising NetOps, the roles and responsibilities of NetOps organizations and key positions, and resources, this paper will next present the facets of NetOps command and control (C2), NetOps linkage to national level strategies and net-centric warfare, and methods to operationalize and integrate NetOps in DoD. Finally, this paper will provide major recommendations to pave the way ahead for the future of NetOps.

NetOps Defined

The first step for DoD to develop a strategy to operationalize and integrate global NetOps is to define and provide a basic understanding of NetOps. Essentially NetOps is the key enabler for electronically sending, receiving, storing, and securing information in DoD. Understanding NetOps begins with the Global Information Grid (GIG). The GIG provides the physical means of communications and computer systems and associated services, along with appropriate software, and the procedural construct for the transport of information using those systems and services. More simply, the GIG involves the systems (hardware and software), processes, and supporting people to move information. All DoD owned and leased communications and computer systems, all software applications, security services, and associated end-to-end information capabilities comprise the GIG.[2]

To provide some perspective to the enormity of the GIG, DoD has "roughly 10,000 computer systems--2,000 of which are "mission-critical"…"[3] and "DoD networks are complex, with over three million computers and a wide variety of operational configurations."[4] Also, it is noteworthy that around 95 percent of U.S. military communications travel over commercial telecommunications networks.[5]

To provide an analogy, if compared to a human body, the GIG would be the circulatory and nervous systems providing the avenues for the transport of essential nutrients and impulses (representative of information), and NetOps would be the brain, controlling these functions. More to the point, NetOps is the overarching construct for operating and defending the GIG. The NetOps construct includes organizations, tasks, procedures, functions, and command and control structure to support all DoD missions.[6] Moreover, NetOps directly supports net-centricity, ensuring the proficient transport and collection of information over the GIG to produce common, relevant operational pictures and global situational awareness.[7]

Drilling down a step further in detail, NetOps involves the integration of the three primary tasks required to operate and defend the GIG--GIG Enterprise Management (GEM), GIG Network Defense (GND), and Information Dissemination Management/Content Staging (IDM/CS). These three functions are not merely separate systems working together in parallel; they are truly interdependent, creating a holistic synergy.[8]

Although interdependent and reliant upon each other, each of the three functions serves a specific purpose for NetOps. GIG Enterprise Management (GEM) provides the means for NetOps. In the body analogy, GEM provides major organs, nerves, muscles, and hormones of the NetOps system. More technically, GEM is defined as "the technology, processes, and policy necessary to effectively operate the systems and networks that comprise the GIG."[9]

Further, GEM is the "day-to-day management (fault, configuration, performance, planning, etc.) of communications (terrestrial and space), electromagnetic spectrum, computer-based information systems, elements of systems, and services to include software applications."[10] Also formerly known as systems and network management (S&NM), GEM is the most technical aspect of NetOps.

Information Dissemination Management/Content Staging (IDM/CS) is the "message" portion of NetOps, or analogous to the brain neurons and cells, which have stored information and are used to direct action in the human body. It is the least concrete portion, and is mostly about tactics, techniques, and procedures. IDM/CS is defined as the "technology, processes, and policy necessary to provide awareness of relevant, accurate information; automated access to newly discovered or recurring information; and timely, efficient and assured delivery of information in a usable format."[11] IDM/CS is central to the overall NetOps theme of providing the right information to the right people at the right time in the right context, "while optimizing the use of information infrastructure resources. IDM/CS provides services that address awareness, access, and delivery of information."[12] IDM/CS provides the most direct common user interface with NetOps, and is important to help zero in on the nugget of crucial information that may be buried in the vast mountain of data available.

GIG Network Defense (GND) protects both the "means" of NetOps, GEM, and the "message" of NetOps, IDM/CS. The analogy here is clearly to the body's immune system. GND provides the full range of information protection, including Computer Network Defense (CND), Information Assurance (IA), and the network aspects of Critical Infrastructure Protection.[13] GND "ensures the availability, integrity, identification, authentication, confidentiality, and non-repudiation of friendly information and information systems while denying adversaries access to the same information/information systems."[14] The value of NetOps GND is in providing a comprehensive level of security so warfighters and decision-makers can trust the information they use to command, control, and conduct combat operations, as well as day-to-day missions.

Roles and Responsibilities

Given the broad extent of NetOps, and its critical function to enable the effective and secure transport of information to all warfighters and decisionmakers, it is important to know who is involved and define their responsibilities. Commander, U.S. Strategic Command (CDRUSSTRATCOM), clearly has the leading role for NetOps in DoD, as assigned by the Secretary of Defense (SECDEF). The Unified Command Plan (UCP), dated March 2005, assigns CDRUSSTRATCOM as the responsible Combatant Commander for Information Operations (IO) and global command, control, communications and computer systems (C4), intelligence, surveillance, and reconnaissance (C4ISR).[15] Concomitant with this assignment, "CDRUSSTRATCOM has determined that this mission includes directing Global NetOps operations; advocating the NetOps requirements for all COCOMS [Combatant Commands]; and planning and developing national requirements."[16]

Although CDRUSSTRATCOM has the overall lead for NetOps, the day-to-day direction and implementation of NetOps is delegated to the Commander, Joint Task Force-Global Network Operations (JTF-GNO). The Secretary of Defense (SECDEF) has assigned the role of Commander, JTF-GNO to the Director, Defense Information Systems Agency (DISA).[17] The authorities and responsibilities under this dual hat arrangement establish the foundation for global NetOps execution.

In order to move forward with a DoD strategy to provide operational relevance and integration of NetOps, CDRUSSTRATCOM must take the lead. However, the "ownership" of NetOps and the information it enables is not clear cut. For example, each warfighting geographic Combatant Command expects to control and "own" information in their theater and each military service expects to manage the networks they pay for, build, and maintain. In addition, the Office of the Secretary of Defense, Joint Staff, and other agencies have a stake in global NetOps as well. To clarify, these higher level roles and responsibilities beyond CDRUSSTRATCOM will be described in greater detail.

In general, all Combatant Commands, Services, and Agencies (CC/S/A) have the role and responsibility of controlling and implementing their portions of the GIG, developing policies and procedures to ensure global interoperability, and supporting USSTRATCOM for NetOps events that have a global impact.[18] The CC/S/As are also responsible for incorporating NetOps into their own command, service, or agency directives and training plans.[19]

More specifically, the Geographic Combatant Commands (GCCs) exercise "OPCON over the GIG assets in their theater and Component NetOps forces.... [and] have the authority to direct efforts and actions that affect the portions of the GIG in their AORs."[20]

Also, Functional Combatant Commands (FCCs), with their global missions, have their own GIG assets and networks (e.g., SCAMPI, Joint National Training Capability, Global Transportation Network, and Ballistic Missile Defense) for which they are responsible.[21] While FCCs are often supporting to GCCs, they still exercise operational control over their portions of the GIG.[22]

In addition, the military Services (U.S. Army, Navy, Air Force, Marines) have the responsibility for "organizing, training, equipping, and providing forces to fulfill specific roles and for administering and supporting these forces."[23] However, these Service responsibilities are "subject to the combatant commander's authority to organize assigned forces and ensure their preparedness as necessary to accomplish a specific mission."[24]

At the DoD level, the Assistant Secretary of Defense (Networks and Information Integration) (ASD(NII)), as the DoD Chief Information Officer, has prime responsibility in the area of NetOps. The ASD(NII) is required to direct GIG planning, architecture development, and implementation. In addition, this position has responsibility for providing a DoD-wide framework for a joint, integrated systems architecture that all services and agencies must build toward, and to enforce compliance with National Security Systems and information assurance requirements. Finally, the ASD(NII) seeks to minimize needless information technology and systems duplication, and recommends DoD GIG requirements to the Joint Requirements Oversight Council.[25]

At the Joint Staff level, the Chairman of the Joint Chiefs of Staff (CJCS), acts as the "spokesman for the combatant commanders, especially on the operational requirements of their commands"[26] and is "responsible for developing joint policy for the end-to-end operational network policies and overall direction of the DoD GIG networks."[27] Functionally, the Joint Staff Director for Command, Control, Communications, and Computer Systems (J6) has authority for "operational DoD GIG Networks' Operations policy and direction"[28] and "shall adjudicate the apportionment and allocation of GIG assets between [Combatant Commands] and Services, as necessary."[29]

The Director, National Security Agency (NSA), is also dual hated as the USSTRATCOM Joint Functional Component Commander for Network Warfare (JFCC-NW). In this role, he is responsible for "planning, integrating, and coordinating computer network warfare capabilities and integrating with all necessary computer network defense and exploitation capabilities. …This includes development of information/intelligence support and information assurance requirements for supporting network warfare…and direct coordination with JTF-GNO."[30] This is significant, since this demonstrates a distinct overlap in the area of computer network defense between JTF-GNO and JFCC-NW. NSA also is responsible to provide "IA products, solutions, and services…[and] will serve as the National Manager responsible to the Secretary of Defense for the security of telecommunications and information systems…"[31] among several other NetOps related technical tasks.

The Defense Intelligence Agency (DIA), has NetOps functional responsibility for intelligence systems, particularly the Joint Worldwide Intelligence Communications System (JWICS). DIA is responsible for "developing, implementing, and managing the configuration of information, data, and communications standards for intelligence systems…"[32]

Also, the Defense Agencies (for example, Defense Logistics Agency, Defense Threat Reduction Agency, etc.) have a significant role in NetOps since they establish, operate, and maintain their own supporting networks and have resources that are still a part of the overall GIG. This means they need to be actively involved, and through their perspective of their GIG assets provide support to global NetOps.[33] Additionally, the Director of National Intelligence (DNI), while not at this time directly part of DoD NetOps, has an agreement for the Intelligence Community-Chief Information Officer (IC-CIO) to work with the DoD CIO to share NetOps status information and to develop joint procedures for IC Networks.[34]

The roles and responsibilities for NetOps are obviously far ranging and multifaceted. USSTRATCOM's leading role is by no means cut and dry or definitive. Also, given the interconnectedness of global networks, and the potential global impact of local actions and disruptions, clear lines of authority and responsibilities across DoD are necessary. Unless all these organizations are brought under single DoD direction, and develop a common understanding of responsibilities, then there is great risk in actions being taken by one that can unintentionally adversely affect others.

Resources

All of the above commands, services, and agencies employ resources in their roles and responsibilities. These resources provide the means for the strategy to operationalize and integrate NetOps in DoD. The primary resource in any government activity is people. The most readily apparent group of people involved is the idea of a NetOps Community of Interest (COI). The NetOps COI has a "shared objective and mission to operate and defend the GIG" and describes "the collaborative group of organizations responsible for operating and defending the GIG."[35] The NetOps COI is comprised of all organizations that employ or in some way interact with the GIG to accomplish NetOps, including organizations from "the Office of the Secretary of Defense, Joint Chiefs of Staff, Combatant Commands, Military Services, Defense Agencies, Other U.S. Government Agencies, IC [Intelligence Community], coalition partners, and NGO [non-governmental organizations]."[36] This goes beyond just DoD, and it further makes sense to include designated Allies, where we have a long-standing formal agreement or partnership.

Coalition partners and NGOs, where we normally have relatively short-term partnerships and goals, are involved in the COI mostly dependent upon specific missions and situations.

The primary people considered in the organizations of the NetOps COI are the information technology (IT) professionals, technicians, and experts. These people apply their detailed knowledge and expertise to provide the actual means for the delivery and protection of information, and are prepared to adapt to the complexity of technological systems. NetOps COI people focus on technological solutions, such as network management programs and information assurance toolsets. However, this emphasis does not adequately recognize the need for *all* DoD individuals to: protect information when it is resident outside computer networks; prevent the disclosure of certain information to the wrong people; and identify each of the pieces of "right" information, "right" timing, and "right" recipients. Everyone in DoD has a function in NetOps, so the people involved are more than just the leaders of the COI organizations, and more than the thousands of IT professionals. NetOps provides a service and is essential to the daily missions of everyone in DoD. This distinction is important since any NetOps direction and strategy must apply to all in DoD and the COI.

The GIG, as defined above, includes all DoD network systems, communications systems equipment, transmission media and apparatus, software, security devices, computers, and the like, providing the second set of NetOps resources.[37]

The final ingredient to NetOps resources is funding. Considering the people involved in NetOps (even just those leaders and "technicians" directly involved) and the extent of the GIG networks, systems (terrestrial and space), equipment, devices, software, etc., the overall DoD NetOps budget is on the order of several billion dollars per year. Indicative of the scope of the dollars involved, the costs for a few GIG initiatives are: $383M (FY04) for GIG Bandwidth Expansion;[38] $682M (FY05 and increasing to about $1.3B in FY08) for Joint Tactical Radio System (JTRS);[39] $530M (FY05 and increasing to about $2.1B in FY09) for Transformational Communications Satellite (TSAT);[40] and $213M (FY05) for Horizontal Fusion.[41] Additionally, the overall DoD budget estimate for Command, Control, and Communications (C3)-related operations and maintenance (all four Services) for FY06 alone is $4.8B.[42] The funding for NetOps, which encompasses most C3 activities, is a non-trivial portion of the annual DoD budget.

The span and scale of all NetOps resources is staggering. In a fiscally constrained, yet increasingly complex and uncertain environment, with myriad threats from conventional to catastrophic, it behooves DoD to establish a strategy that brings all related resources together to deliver efficiencies and eliminate redundancies. A lack of unified direction and consolidation could force cuts in individual areas adversely affecting operations.

NetOps Command and Control

Joint Publication 0-2, *Unified Action Armed Forces*, states "command (the lawful authority of a commander) and control (the regulation of forces and functions to accomplish the mission in accordance with the commander's intent) is the most important function undertaken by a JFC [Joint Force Commander]."[43] While NetOps provides the mechanism and means for effective DoD command and control (C2), this section will review the current C2 for the implementation and execution of NetOps itself.

Gen James Cartwright, CDR USSTRATCOM, asserts the "Joint Concept of Operations [CONOPS] for Global Information Grid NetOps" document, known as the NetOps CONOPS for short, describes the "common framework and command and control structure that we [NetOps community, defined in the next paragraph] will use to conduct the global NetOps mission…"[44] In addition, NetOps C2 process involves commanders executing required functions to ensure effective GIG operations.[45] That said, there are several facets to NetOps C2—the operating principles, collaborative C2 process, and the C2 structure, which have both global and theater elements.

The first facet includes the NetOps C2 operating principles. These principles are rooted in "Information Age C2" as opposed to "Industrial Age C2" as described in the DoD "Joint Command and Control Functional Concept."[46] Information Age C2 is a dynamic, decentralized, and highly adaptive joint decisionmaking process enabled by a collaborative information environment.[47] It will allow for tailoring of systems and procedures, and achieve timely initiative without sacrificing unity of effort or required coordination.[48]

As described in the USSTRATCOM NetOps CONOPS, "as a critical enabling capability to achieving net-centricity, NetOps must adopt Information Age C2 structures and processes."[49] Given this Information Age C2 construct, the principles for NetOps C2 include GIG self-synchronization, execution at the lowest level of command possible, and the consideration by all commanders of the potential global impact of their actions.[50]

The next facet is the collaborative NetOps C2 process, also primarily based upon the DoD Joint Command and Control Functional Concept, "used to coordinate the development of decisions and actions across multiple basic C2 process"[51] loops. "Commanders need to be able to share their observations, understanding, decisions, and actions regarding a situation with other commanders. Collaborating allows commanders to get better situational awareness, a deeper understanding of the operational environment, to better comprehend how their decisions will effect the operational environment and to coordinate their limited resources with others to achieve maximum effect in the pursuit of mission success. Collaboration is enabled through a collaborative information environment (CIE)."[52]

Further, the NetOps CONOPS states collaborative NetOps C2 will achieve GIG unity of effort, with swift and flexible synchronization and decisionmaking, along with shared understanding of commander's intent, yet not sacrificing unity of command.[53]

Finally, the NetOps C2 structure has two main parts—Global NetOps C2 and Theater NetOps C2. The supported commander for Global NetOps C2 is Commander, USSTRATCOM, who directs the other COCOMs, Services, and Defense Agencies to ensure GIG availability and integrity.[54] Although functioning as supporting commands, the other COCOMs still retain their DoD authority over assigned NetOps forces.[55] The JTF-GNO directs global NetOps C2 on behalf of USSTRATCOM, and has operational control (OPCON)[56] of Service NetOps units.[57]

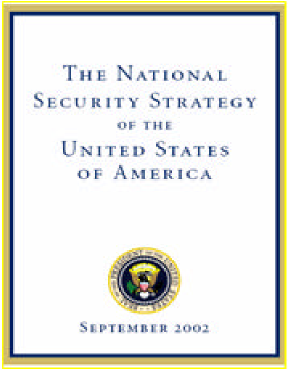
The Geographic COCOMs are the supported commands for Theater NetOps C2, and have the "authority to direct efforts and actions that affect the portions of the GIG in their AORs."[58] USSTRATCOM (along with JTF-GNO), the Functional COCOMs, Services, and Defense Agencies are in a supporting role, and will help ensure GIG capabilities can meet requirements.[59] JTF-GNO is responsible for de-conflicting resource requirements when contention arises between COCOMs, and those that "cannot be resolved will be forwarded through CDRUSSTRATCOM to the CJCS for adjudication."[60]

A situational NetOps event provides the determining factor for global versus theater NetOps C2. An event is the "collective term for all NetOps activities that have the potential to impact the operational readiness of the GIG."[61] This distinction provides for global operation of the GIG, but allowing Geographic COCOMs to direct NetOps actions in their theaters.[62] A Global NetOps event has the "potential to impact the operational readiness of the GIG and requires a coordinated response amongst affected Combatant Commanders, Military Services, Defense Agencies, and other members of the NetOps COI."[63] Meanwhile, a Theater NetOps event occurs within theater and has the "potential to impact the operations in the [affected] theater."[64]

Considered holistically, the operating principles, collaborative process, and the global/theater structure, define NetOps C2. This provides a new "Information Age" construct to obtain unity of effort amongst the NetOps COI, and ensure the GIG provides relevant, timely, and secure information to warfighters and decisionmakers. However, unless DoD adopts a commonly understood NetOps C2 construct that provides true unity of effort, then network "fratricide" is a distinct possibility.

Linkage to Higher Level Strategies and Net-Centric Warfare

An operational DoD-level strategy to operationalize and integrate NetOps must have direct linkage to higher level national strategies. This linkage is a necessary first objective in any DoD strategy to ensure NetOps properly supports overall DoD goals and objectives, as well as national security goals and objectives.



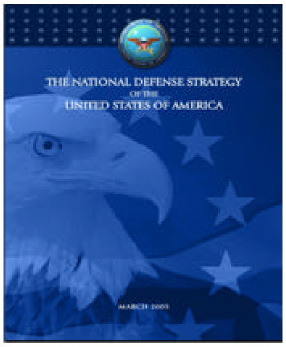
THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA

SEPTEMBER 2002

Figure 1

The National Security Strategy (NSS) is the top-level national strategy document which provides the foundation for defense policy and strategy. NetOps, given its primary role in the defense information realm, can cover the entire range of strategic goals and interests discussed in the NSS. However, an initial linkage for defense information policy can be derived from "meeting the challenges and opportunities of the twenty-first century," and the mention of required military capability to "conduct information operations…and protect critical U.S. infrastructure…"[65]

The National Defense Strategy (NDS) provides the initial context for national defense information, and directly cites "conducting network-centric operations" as a key operational capability.[66] The NDS states the U.S. "will conduct network-centric operations with compatible information and communications systems…" in order to "increase efficiency and effectiveness across defense operations…by giving all users access to the latest, most relevant, most accurate information."[67] These capabilities and attributes in the NDS provide a direct linkage for a DoD NetOps strategy.

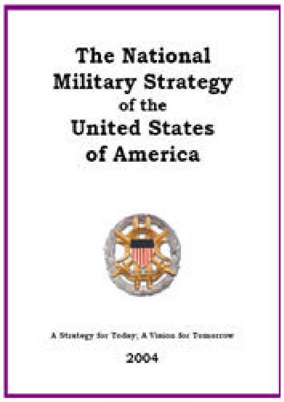


THE NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA

MARCH 2005

Figure 2

The National Military Strategy (NMS) provides further guidance on NetOps policy. Specifically relevant are the NMS functions and capabilities of "Securing Battlespace" and "Achieving Decision Superiority" as elements of "A Joint Force for Mission Success."[68] Additionally, as NetOps is the operational construct to operate and defend the GIG, it is especially noteworthy the NMS has the GIG as one of only five initiatives directly mentioned. The NMS asserts "the GIG has the potential to be the single most important enabler of



The National Military Strategy of the United States of America

A Strategy for Today, A Vision for Tomorrow

2004

Figure 3

information and decision superiority" and discusses the GIG role in ensuring "information and knowledge for decision-making; technical, policy, and organization issues; and innovative capabilities."[69] Global Network Defense (including Information Assurance), as a prime element of NetOps in DoD, is a significant element of securing battlespace. Information and C4 architectures are definitely within the scope of responsibility of NetOps, and provides a specific linkage point for a DoD NetOps strategy.

The National Strategy to Secure Cyberspace (NSSC) provides "direction to the federal government departments and agencies that have roles in cyberspace security"[70] and has direct relevance, since NetOps provides the key role in DoD cyberspace security. Also, NetOps provides the primary mechanism for DoD to support the strategic objectives of the NSSC, namely "prevent cyber attacks against America's critical infrastructures; reduce national vulnerability to cyber attacks; and minimize damage and recovery time from cyber attacks that do occur."[71] NetOps further specifically ties to the NSSC, which "identifies steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity"[72] since as mentioned earlier, DoD employs commercial networks for about 95 percent of U.S. military communications.[73]

THE NATIONAL STRATEGY TO SECURE CYBERSPACE

FEBRUARY 2003

Figure 4

Another key objective for NetOps is to serve as the "essential enabler for the GIG to achieve the net-centric warfare [NCW] goals."[74] One of the key elements of the DoD strategy for the implementation of NCW is to "accelerate deployment of network-centric systems, concepts, and capabilities: As new network-centric systems, concepts, and capabilities are developed by the Services and Combatant Commands, they should be deployed to the units and geographical areas where they can be refined and employed when needed."[75]

NetOps must nest within the scope and focus of the national-level strategies since they are fundamental to guiding all DoD operations. While the case can be made for some NetOps linkage to these national-level strategies, in many cases it is too tenuous. Incorporating a strong link to NetOps in future versions will emphasize the critical nature of NetOps, and set the stage for a DoD NetOps strategy.

Operationalizing and Integrating NetOps

Operationalizing and integrating NetOps is essential to ensure a common focus and understanding of information needs across DoD. These are the criteria for ensuring NetOps success. This move will further provide a direct connection to DoD warfighting capabilities, and help convey the appropriate significance of NetOps to all warfighters and decisionmakers…not just the technical experts who build and manage the physical communications networks and systems. Combatant commanders rely on NetOps to provide the means for their command and control capabilities, situational awareness, and information flow…without NetOps, combat aircraft don't fly, tanks don't move, ships don't sail, and satellites don't provide information. This is the essence of "operationalizing," to affirm the direct warfighting capability and significance, on par with joint fires, precision strike, etc. To underscore the relevance, as President Bush announces in the National Strategy to Secure Cyberspace, "the way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependent network of information technology infrastructures…"[76]

Moreover, the Joint Staff's Joint C4 Campaign Plan discusses "operationalizing the GIG" as an essential part of maximizing its performance and making it "more responsive to the Joint Force," thus helping to achieve information superiority. [77] NetOps, which drives the GIG, must be centered on operations to provide effective joint force capability. An operational focus ensures commanders have the proper appreciation and wherewithal, that is the situational awareness, to visualize and influence warfighting information to optimize their mission execution.

Integrating NetOps means a cohesive combination of all its elements, namely GEM, GND, and IDM/CS, to achieve operational synergy. This is highlighted in the Capstone Requirements Document (CRD) for the GIG asserting "to effectively support network-centric warfare (including collaborative planning) key parts of these functions [GEM, GND, and IDM/CS] must be integrated. Commanders (e.g., at the theater and enterprise level) must have situational awareness of network IT assets and the information flow across echelons."[78] Also at the technical level, it means providing a common focus for the myriad of network initiatives across the DoD, including all information systems programs of the services and Defense Information Systems Agency, such as GIG Enterprise Services (GIG ES),[79] and the Transformational Communications Architecture.[80]

Effective integration of NetOps capability into the full range of military operations is another key factor. Relating to NetOps, the previous Commander of DISA, Lt Gen Raduege (now retired), in his testimony to the House Armed Services Committee, said "the integration of military Service and agency-developed data sources and decision support tools is essential to the combatant commanders' ability to "fight jointly.""[81] Additionally, the DoD Joint Operations Concepts states "the Joint Force must move beyond deconfliction to fully *integrated* [emphasis added] elements with all functions and capabilities focused toward a unified purpose."[82] Relating to NetOps, the Joint C4 Campaign Plan says "our goal is to better *integrate* [emphasis added] and synchronize joint C4 efforts…[while] transformation to network centric operations is one of the most complex, difficult, and far-reaching initiatives ever attempted."[83] Although integration is a distinct challenge, it is also a prerequisite to achieve decision superiority.

Integration is essential to interdependence, and leads to interoperability as well. The need for NetOps to accomplish these three "i"s is important to attain maximum overall combat capability. Interdependence develops otherwise unrealized synergies where the whole is greater than the sum of the parts. The Net-Centric Environment Joint Functional Concept describes interdependence as "…a mode of operations based upon a high degree of mutual trust, where diverse members make unique contributions toward common objectives and may rely on each other for certain essential capabilities rather than duplicating them organically."[84] Lt Gen Raduege, previous Commander, DISA provided more on the case of interoperability, when he testified "interoperability is the core of jointness" and interoperability of weapon systems, sensors, and tactical assets, along with their imbedded C4 capabilities is prerequisite to achieve gains in precision and timely operational capability. [85]

Much needs to be done to obtain full spectrum NetOps integration, interdependence, and interoperability. The first goal in the Joint C4 Campaign Plan, to "transform joint, multinational, and interagency C4 warfighting capabilities to maximize combat effectiveness,"[86] points out the requirement for interagency and multinational integration.

Operationalizing and integrating, along with effective interdependence and interoperability, will place NetOps squarely into the forefront of warfighting where it belongs. The global power, reach, and presence of DoD demands accessed, coordinated, correlated, fused, shared, and protected information provided through operationalized and integrated NetOps. These criteria provide the basis for a pertinent and achievable NetOps strategy.

Way Ahead

A strategy with balanced ends, ways, and means is essential to operationalize and integrate NetOps in DoD. Given the current background and focus of NetOps, DoD must take several challenging actions to set the stage for 21st century net-centric warfare and fly toward full battlespace dominance:

1) Include the concept of NetOps in the next versions of national-level strategies, in particular the NMS and NSSC. NetOps should be included as a key enabler for Securing Battlespace and Decision Superiority in the NMS, and should further cite NetOps, vice the more specific GIG, as the initiative relevant to the Joint Vision for Future Warfighting. NetOps terminology and functionality should also be addressed in the NSSC, since the NetOps community goes beyond just DoD. NSSC actions and recommendations should consider NetOps, particularly the security aspects, and maintain consistency with DoD direction. This will pave the way for synchronized coordination and effort between DoD, other federal government agencies, industry, and every applicable element of society.

2) Develop a common set of NetOps goals and objectives across DoD. The development of NetOps systems must move toward common goals, integrated into DoD operations, and meet warfighter needs. This common set would bring together the currently disparate NetOps goals and objectives outlined in several documents, including ASD(NII)/DoD CIO goals statement, the Joint C4 Campaign Plan, the Joint Transformation Roadmap, the Capstone Requirements Document (CRD) for the GIG, ASD(NII)/DoD CIO and JS/J6 memo, DoD Data Strategy, Net-Centric Warfare, as well as others focused on information and network/communications systems. The ASD(NII) and CDRUSSTRATCOM, as the DoD leading authorities for NetOps, must develop one set of common goals to provide universal overarching direction and focus, and provide a construct to balance these ends with ways and means.[87]

3) Manage NetOps as a weapons system. While net-centric warfare takes on increasing importance as a key enabler for conducting the full range of military operations, the DoD must develop the capability to optimize the dependability and flexibility of information systems, networks, and information assets. Managing network operations as a weapons system[88] allows proper focus on ensuring information availability and effective employment as a force multiplier. Also, the network weapons system is constantly employed, consistently requiring effective network defense in depth, as systems under cyber attack at all times, unrelenting. This concept in the related field of intelligence, surveillance, and reconnaissance (ISR) was recognized as well in Operation Iraqi Freedom lessons learned. An Army Intelligence Center report stated the "proper allocation of ISR assets is a combat multiplier when treated like a weapons system—

one that must focus at the point of decision, and dynamically retask as the situation changes."[89] Conducting NetOps as a weapons system will drive progress toward a common, integrated system, avoiding "stovepipes" and unsupportable "drive-by fieldings" (a concept fairly well known within many communities in all four Services, where a system or equipment item is mandated by higher headquarters and delivered without appropriate associated training, resources, logistics supportability, etc).[90] In addition, the weapons system perspective will drive NetOps toward the necessary "simpler is better" approach, including a "critical capability for the network to self-form and self-heal to fill gaps created during the course of military operations" as described in the Joint C4 Campaign Plan.[91] NetOps is not an operational end in and of itself…it cannot be a "self-licking ice cream cone"…its significance comes from the guaranteed provision of information. Conducting NetOps as a weapons system will ensure the focus on warfighting information and not self-serving technical elements.

4) The Secretary of Defense, with Congressional authority, must provide the Commander, USSTRATCOM, the authority and responsibility over all NetOps funding and programs. This authority would be similar to U.S. Special Operations Command (USSOCOM)'s for special operations forces. This represents a significant shift from the current DoD paradigm of the military Services controlling all funding and programs. Provision of DoD-wide NetOps-related funding and development is the only consistent and reliable method to ensure unified, common direction with appropriate governance and warfighting focus. The Office of the Secretary of Defense, specifically from ASD(NII) and the Joint Staff, would provide oversight. This need for centralized accounting is recognized by Dr. Wells, ASD(NII), and LtGen Shea, Joint Staff/J6, by stating in their memorandum to Combatant Commanders and the Services, "presently disjointed approaches for identifying, acquiring, testing, evaluating, integrating, and fielding joint C4 capabilities need to be coordinated. …New governance approaches and effective systems engineering of both the overall Global Information Grid (GIG) and of individual programs are essential."[92] This approach further best addresses Joint Transformation Roadmap requirements.[93]

This new and far-reaching advance puts a warfighting Combatant Commander in charge of acquiring vital assets, and can pave the way for one "born joint" network, vice the current conglomeration of several different service, agency, and command networks. This approach further tackles head on the myriad of challenges outlined by Mr. John Gentry in his *Parameters* article, "Doomed to Fail: America's Blind Faith in Military Technology," particularly "the lack of centralized accounting," "the fractured design and control of DoD's IT infrastructure creates opportunities for attackers," the services and Defense agencies continuing to buy systems for only their own use and not for joint purposes, and non-compliance with the Clinger-Cohen Act of 1996.[94]

5) The ASD(NII) and Joint Staff should establish a directing Council with flag officer representation from all the COCOMs, Services, and Defense Agencies. Commander, USSTRATCOM should lead this Council, with oversight from ASD(NII) and Joint Staff. This responsibility must not be delegated by USSTRATCOM to a lower level, such as the JTF-GNO, which is tied at the hip with DISA. It must be top-level command authority, with oversight by the Joint Staff. Also, other federal agencies (especially Department of Homeland Security, Department of State, Department of Justice, and Department of Commerce among others), allies, and the commercial sector should have associate representatives on the Council. This council would review, prioritize, and direct NetOps funding across the DoD. The current system of the Services developing, providing, and funding combat systems for the warfighting Combatant Commands is adequate where "jointness" or "interoperability" is really at the procedural or conceptual level. When it comes to airplanes, tanks, and ships, these physical assets simply do not operate in the same battlespace. However, NetOps requires total integration and interoperability. The NetOps Council is the one and only way to ensure a constant warfighting focus for NetOps, a proper balance between current warfighting needs, and long-term program development. This represents the reality of cyberspace, where integration and interoperability are especially relevant and critical. The Council will specifically address and resolve the issue of "the DoD…electronic system-based force structure is expensive, fragile, and vulnerable, but system architectures are not easy to change. Rapidly evolving technology and the independent decisions of members of the DoD confederacy assure that enterprise-wide interoperability will not occur soon."[95] This Council will further provide a single avenue for DoD to coordinate and further combine efforts with other government agencies, allies, and the private sector. While non-DoD members (other government agencies, commercial sector, coalition allies, etc.) are mentioned as part of the NetOps COI, there must be a well defined, clear linkage. This linkage must support a unity of effort, with common understanding and common purpose.

6) USSTRATCOM must establish a NetOps C2 structure with clear unity of command as well as unity of effort. NetOps is perfect for adapting to a new "Information Age" C2 construct, but while striving to transform for the future, current realities must be taken into account.
JP 0-2, UNAAF, has "simplicity" as a principle for organizing joint command and control. This includes an "unambiguous chain of command, well-defined command relationships, and clear delineation of responsibilities and authorities."[96] JP 0-2 also asserts "command is central to all

military action, and unity of command is central to unity of effort."[97] In particular, USSTRATCOM must eliminate the duality of global vs. theater events and C2 structures, and clarify computer network defense (CND) roles and responsibilities between JTF-GNO and the NSA as the JFCC-NW. Given the interconnectivity and global nature of NetOps, there are very few exceptions to considering every NetOps event as "global." To ensure the primacy of warfighting operations, the single NetOps C2 structure should recognize the GCCs as supported, yet following global commander's intent provided by Commander, USSTRATCOM. The Unified Command Plan assigns a GCC to every part of the globe, so there are no geographic seams in execution. The GCCs obviously know best their areas of responsibility, their missions, and the impact of NetOps events.

7) JTF-GNO should take complete lead responsibility for Computer Network Operations (CNO). This will resolve the current duality of both JTF-GNO and NSA having responsibility for CND. That is, JTF-GNO with CND responsibility as part of NetOps, and NSA with CND responsibility as part of CNO. An alternate solution of just "removing" CND from either NetOps or CNO is not feasible since it is intimately intertwined with both. JTF-GNO is best suited to take on the complete CNO mission given its primary mission focus on NetOps and computer systems in general, along with the range of capabilities and knowledge-base they can bring to the table, especially in partnership with their dual-hat with DISA. NSA should be a coordinating and supporting organization, with its primary focus on intelligence activities.

8) USSTRATCOM, with USJFCOM supporting, must establish and lead a robust training and education program. There must be different levels of the training common to all Services, COCOMs, and Defense Agencies. The first and most technical level needs to be geared toward the NetOps "crew" which is responsible for the actual conduct and implementation of NetOps elements, including network management and network defense. Another level of training must be geared toward DoD warfighters and leaders, with a focus on NetOps capabilities, limitations, and how it integrates in combat operations. Although the Services are responsible for training, a common set of training standards and methods is essential to realize NetOps commonality and unity of effort. As a supporting effort, "the U.S. Joint Forces Command will develop Joint TTPs [tactics, techniques, and procedures], Programs of Instruction..."[98] This focus provides the avenue to deliver on the DoD Joint Operations Concepts, which maintains "people remain the centerpiece of successful joint operations."[99]

9) Develop and conduct robust NetOps exercises and drills. As the Joint C4 Campaign Plan points out, "exercising and refining the Joint GIG NetOps Concept of Operations (CONOPS)"[100] is a major objective to meet the goal of transforming capabilities to attain

optimum warfighting effectiveness. U.S. Joint Forces Command (USJFCOM) should develop and lead this effort, with guidance and direction from U.S. Strategic Command, the other COCOMs, Services, and Joint Staff. Exercises are a common responsibility assigned to USJFCOM in the Unified Command Plan, and explicitly stated in the USJFCOM Joint Transformation Roadmap.[101] There should be at least one major, global NetOps exercise per year, along with one or two minor specific theater event exercises. The focus should be on practicing and developing common tactics, techniques, and procedures, testing interoperability, improving the speed of information flow, and restoring services.

10) Finally, build a DoD NetOps overarching strategy that balances ends, ways, and means. This will provide common, well understood NetOps direction across the Department, and establish a common interface with other agencies, allies, and commercial sector. Universal NetOps standards specifications, and enforcement methodologies would further flow from the strategy. The only constant in warfighting is change, and in order to effectively adapt to operational mission requirements, commanders must understand NetOps performance and capabilities (as well as limitations), and have the ability to dynamically and cohesively posture NetOps to employ the right information to obtain the desired winning effects. A cohesive strategy is a prime necessity to truly build directly toward information superiority and realize the benefits of decision superiority. Ideally the strategy would employ methods to operationalize and integrate NetOps as discussed, and include appropriate roles, responsibilities, and resources.

Conclusion

This flight plan toward a DoD strategy to operationalize and integrate Global NetOps will enable assured, timely, and relevant information to the right warfighters and decisionmakers at the right time in the right context. NetOps provides the central “engine” that drives the Information element of national power in the DoD. As Joint Publication 1, *Joint Warfare of the Armed Forces of the United States,* states:

> “information itself is a strategic resource vital to national security. This reality extends to the Armed Forces at all levels. Military operations in particular are dependent on many simultaneous and integrated activities that, in turn, depend on information and information systems. Information and information-based technologies are vital elements for modern war and military operations other than war (MOOTW).”[102]

NetOps is central to communications and defense information, and directly relates across the range of core U.S. national interests.

To ensure NetOps provides for the fundamental information to reach the right people at the right time, in the right context, DoD must take several actions. These include providing clear linkage to national strategies; develop a single set of NetOps goals and objectives; approach NetOps as a weapons system; provide Commander, USSTRATCOM, the authority and responsibility over all NetOps funding and programs; establish a NetOps Council to execute this funding authority and responsibility; establish a clear NetOps C2 construct to obtain real unity of effort with solid unity of command; assert JTF-GNO responsibility for all computer network operations; provide realistic and germane NetOps training and education; and develop robust exercises and drills to "test" NetOps. Conclusively, all these actions must be brought together, and a DoD NetOps strategy built that focuses direction and balances ends, ways, and means. This approach will certainly experience turbulence, uncertain weather, and unforeseen full spectrum threats, but the only greater risk is not reaching the destination, which is providing the best assurance possible to fighting and winning all our nation's wars and conflicts.

Endnotes

[1] Donald H. Rumsfeld, *The National Defense Strategy [NDS] of the United States of America* (Washington, D.C.: n.p., March 2005), 13-14.

[2] U.S. Department of Defense, *Global Information Grid (GIG) Overarching Policy*, DOD Directive (DODD) 8100.1 (Washington, D.C.: U.S. Department of Defense, 19 September 2002, Certified Current as of 21 November 2003), 8 defines the GIG as "the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority."

[3] Arnaud de Borchgrave and et al, *Cyber Threats and Information Security: Meeting the 21st Century Challenge: A Report of the CSIS [Center for Strategic and International Studies] Homeland Defense Project* (Washington, D.C.: CSIS Press, May 2001), xi.

[4] U.S. Joint Staff, Command, Control, Communications and Computer Systems Directorate (J6), "Joint C4 Campaign Plan," September 2004; available from http://www.jcs.mil/j6/c4campaignplan/Joint_C4_Campaign_Plan.pdf; Internet; accessed 28 November 2005, 21.

[5] John A. Gentry, "Doomed to Fail: America's Blind Faith in Military Technology," *Parameters* (Winter 2002-2003, available from http://carlisle-www.army.mil/usawc/parameters/02winter/gentry.htm; Internet; accessed 30 November 2005, 90.

[6] General James Cartwright, Commander, U.S. Strategic Command, *Joint Concept of Operations for Global Information Grid NetOps*, Version 2 (Omaha, NE: USSTRATCOM, 15 August 2005),1, states NetOps is "the operational construct consisting of the essential tasks,

Situational Awareness (SA), and C2 that CDRUSSTRATCOM [Commander, United States Strategic Command] will use to operate and defend the GIG." Also, U.S. Defense Information Systems Agency (DISA), "NetOps," fact sheet available from http://www.disa.mil/go/go3.html; Internet; accessed 15 December 2005, mentions NetOps as consisting of the "organizations, procedures, and functionalities required to plan, monitor, manage, coordinate, secure, and control the GIG infrastructure and its operations in support of DOD's global missions."

[7] DISA, "NetOps" fact sheet, asserts NetOps "provides the technical and operational underpinning supporting the net-centric requirement for producers and consumers of information to efficiently and effectively store and move information within the GIG and to produce relevant Global Situational Awareness operational pictures."

[8] Cartwright, iii.

[9] Cartwright, 5.

[10] U.S. Defense Information Systems Agency (DISA), "Core Services-NetOps," fact sheet available from http://www.disa.mil/main/prodsol/cs_netops.html; Internet; accessed 15 December 2005.

[11] Cartwright, 9.

[12] DISA, "Core Services-NetOps."

[13] Cartwright, 7.

[14] DISA, "Core Services-NetOps."

[15] Cartwright, 15-16.

[16] Ibid.

[17] Cartwright, 16. Note this CONOPS for GIG NetOps also states on page 16, "NetOps is conducted by JTF-GNO, unless otherwise directed by CDRUSSTRATCOM."

[18] CJCSI 6215.03 (DRAFT), A-1 to A-3.

[19] Ibid.

[20] Cartwright, 26.

[21] Cartwright, 34.

[22] Ibid.

[23] JP 0-2, I-9.

[24] Ibid.

[25] DODD 8100.1, 3-4 describes the ASD(NII) role as required to "develop, maintain, and enforce compliance with [Global Information Grid Architecture]…and direct the development of

associated implementation and transition plans; …provide a DoD-wide mission area architecture framework that shall be used by the DoD Components to build integrated operational, technical, and systems architecture views. Ensure that the operational views are integrated across Joint Mission Areas; … Provide recommendations to the Joint Requirements Oversight Council for the development of DoD GIG requirements; … Establish GIG compliance and enforcement mechanisms to achieve IT and National Security Systems (NSS) interoperability and information assurance, while minimizing needless duplication of IT and NSS."

[26] U.S. Chairman of the Joint Chiefs of Staff, *Unified Action Armed Forces (UNAAF)*, Joint Publication (JP) 0-2 (Washington, D.C.: CJCS, 10 July 2001), II-5.

[27] U.S. Chairman of the Joint Chiefs of Staff, *Policy for the Department of Defense GIG Network Operations*, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.03 (DRAFT) (Washington, D.C.: CJCS, xx December 2004), 2. Note while this instruction is not yet published, it is the author's belief the items referenced will not change significantly, and the publication still provides a legitimate, Joint Staff-level reference.

[28] CJCSI 6215.03 (DRAFT), 2.

[29] CJCSI 6215.03 (DRAFT), A-1.

[30] Cartwright, 17.

[31] Cartwright, 38-39.

[32] Cartwright, 39.

[33] Cartwright, 35.

[34] Secretary of Defense Memorandum, "Assignment and Delegation of Authority to Director, Defense Information Systems Agency (DISA)," 18 June 2004, as quoted in Cartwright, 38.

[35] Cartwright, 15.

[36] Cartwright, 15.

[37] DODD 8100.1, 8, more specifically mentions GIG resources include "any system, equipment, software, or service that meets one or more of the following criteria: Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services; Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services; [and] processes data or information for use by other equipment, software, or services."

[38] U.S. Joint Forces Command (USJFCOM), "Joint Transformation Roadmap," 21 January 2004; available from http://www.ndu.edu/library/docs/jt-transf-roadmap2004.pdf; Internet; accessed 15 December 2005, 54-55. GIG Bandwidth Expansion (BE) as described in the Roadmap "will provide a transport system that delivers high-speed internet protocol services to key operating locations worldwide, using leading edge technologies from commercial industry.

GIG-BE will expand bandwidth, allowing the use of more robust information tools such as collaborative applications for C2, and near real time video for ISR applications. GIG BE initiative provides a network "redundancy" that ensures assured access to a reliable network, one with diverse information pathways. Specifically, GIG-BE will connect over 100 key intelligence, command, and operational locations."

[39] Ibid, 55. The Roadmap describes JTRS as "a family of software-defined radios with inherent cross-banding and IP routing capability. … JTRS will provide the communications and networking capability for mobile forces that, together with the GIG-BE and TC initiatives, will enable robust enterprise-wide networking. JTRS will replace virtually the entire current inventory of tactical radios and, ultimately, SATCOM terminals as well. Furthermore, JTRS will have an inherent mobile networking capability that will enable mobile forces to remain connected to an IP network. This will be the primary reachback conduit for non-dispersed mobile forces."

[40] Ibid, 55. The Roadmap describes TSAT as "The space-based segment of the GIG transport architecture [which] will expand current capabilities, extending the network's full capability to mobile and tactical users. It will provide satellite communications capability with greatly increased bandwidth and integrated, multi-agency networking capability. It will incorporate Internet Protocol and laser communications capabilities into the Department's satellite communications constellation."

[41] Ibid, 57-58. The Roadmap states the Horizontal Fusion "initiative is a portfolio program that enables access and use of the data that is available on the network. It is aimed at providing the tools that allow users to identify what data is available, access it, smartly pull and fuse it, and make sense of the data gathered. These tools will require investing in data content and management, as well as the acquisition of commercial applications."

[42] Office of the Secretary of Defense, "Operation and Maintenance Overview, February 2005, Fiscal Year (FY) 2006 Budget Estimates," available from http://www.dod.mil/comptroller/defbudget/fy2006/fy2006_overview.pdf; Internet; accessed 26 January 2006, 113.

[43] JP 0-2, III-13.

[44] Cartwright, ii.

[45] Cartwright, 44.

[46] See U.S. Department of Defense, "Joint Command and Control Functional Concept," February 2004, available from http://www.netcentricfcb.org/workshop1_references/C2FC.doc#_Toc65997480; Internet; accessed 2 January 2006. This document provides "the measurement framework for evaluating the command and control investment options needed to implement Joint C2, and for supporting those investment decisions. This Joint C2 Functional Concept also serves to: Generate thought and discussion about new methods for performing command and control across the range of military operations; Provide the conceptual framework for developing integrated architectures used for analyzing Joint Command and Control capabilities; and Provide the basis for military experiments and exercises. The Joint C2 Functional Concept will lead to force development guidance that would require changes in joint force doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF)."

[47] Ibid, 19.

[48] Ibid, 11, states Information Age C2 will “allow people in large organizations to interact with the directness, informality, and flexibility typical of small, cohesive teams or organizations; allow commanders and staffs to tailor the C2 system as required by quickly assembling cohesive teams and by adopting C2 procedures suited to each situation rather than relying on “one size fits all” procedures; and allow the force to exploit the benefits of decentralization—initiative, adaptability, and tempo—without sacrificing coordination and unity of effort.”

[49] Cartwright, iii.

[50] Cartwright, 14 affirms the principles for NetOps C2 include “…self-synchronized operation of the GIG; …activities will be executed at the lowest level of command possible; DoD NetOps direction will be executed through the Unified Command[s]…using supporting/supported command relationships; the supported commander has the authority to take whatever NetOps action is deemed necessary…and has final decision responsibility; all Commanders must continually consider the possible global impact of their actions;…in time critical situations…action may be initiated prior to collaborating…”

[51] DoD, “Joint Command and Control Functional Concept,” 12-13. “The basic C2 process is the systematic execution of the functions that an individual commander is required to perform in order to recognize what needs to be done and to ensure that appropriate actions are taken. …The basic C2 functions are…Monitor and collect data on the situation; Develop an understanding of the situation; Develop a course(s) of action and select one; Develop a plan to execute the selected course of action; Execute the plan, to include providing direction and leadership to subordinates; [and] Monitor execution of the plan and adapt as necessary.”

[52] DoD, “Joint Command and Control Functional Concept,” 14. Also note page A-1 defines the CIE as “the collaborative information environment is a specified information environment that enables collaborative processes at will between a select group of individuals or organizations. The CIE is a subset of the emerging global information environment. The CIE consists of five elements: Infrastructure (the hardware, software, communication links, and appropriate supporting equipment); People (members conducting activities to gain understanding in the environment); Architecture (the virtual connectivity structure designed to deliver, process, and function); Rules (the customs, laws, procedures and policies that govern behavior in the collaborative environment); and Information (the data representing potential knowledge in the environment).” Note the CIE infrastructure and architecture are resident parts of the GIG.

[53] Cartwright, 44.

[54] Cartwright, 40.

[55] Ibid.

[56] See JP 0-2, UNAAF, III-7 to III-8 and GL-10 for OPCON definition and description. OPCON is “the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission.”

[57] Cartwright, 40.

[58] Ibid, 42.

[59] Ibid.

[60] Ibid.

[61] Ibid, 13.

[62] Ibid.

[63] Ibid, 14.

[64] Ibid, 13.

[65] George W. Bush, *The National Security Strategy of the United States of America* (Washington, D.C.: The White House, 17 September 2002), 29-30.

[66] Rumsfeld, NDS, 14.

[67] Ibid, 13-14.

[68] General Richard B. Myers, Chairman of the Joint Chiefs of Staff, *National Military Strategy of the United States of America: A Strategy for Today, A Vision for Tomorrow* (Washington, D.C.: n.p., 2004),13-18. Noteworthy within the "Securing Battlespace" function and capability, as necessary for joint force mission success, the NMS asserts on page 17 that "military operations require information assurance that guarantees access to information systems and their products and the ability to deny adversaries access to the same. Securing the battlespace includes actions to safeguard information...systems that support the precise application of force…. Securing battlespace ensures the ability of the Armed Forces to collect, process, analyze and disseminate…relevant information that contribute[s] to decision superiority."

[69] Ibid, 22.

[70] George W. Bush, *The National Strategy to Secure Cyberspace [NSSC]* (Washington, D.C.: The White House, February 2003), viii.

[71] Ibid, viii.

[72] Ibid, viii.

[73] Gentry, 90.

[74] U.S. Joint Forces Command (USJFCOM), "Joint Transformation Roadmap," 21 January 2004; available from http://www.ndu.edu/library/docs/jt-transf-roadmap2004.pdf; Internet; accessed 15 December 2005, 62.

[75] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare* (Washington, D.C.: U.S. Department of Defense, 5 January 2005), 12.

[76] Bush, *NSSC*, cover letter.

[77] Joint Staff, “Joint C4 Campaign Plan,” 21.

[78] U.S. Joint Forces Command, C4 Plans, Policy and Projects Division, *Capstone Requirements Document: Global Information Grid*, JROCM 134-01 (Norfolk, VA: USJFCOM, 30 August 2001), 36.

[79] USJFCOM, “Joint Transformation Roadmap,” page 58 describes GIG ES as an “investment portfolio [that] integrates existing and future efforts to develop, acquire, field, operate, and sustain enterprise level IT services supporting the Department of Defense Global Information Grid. This investment portfolio supports ASD-NII’s goal to transform the DoD information environment from broadcast and point-to-point communications to a net-centric environment.”

[80] USJFCOM, “Joint Transformation Roadmap,” page 54 describes the Transformational Communications Architecture as “the transport element of the GIG and will be composed of three integrated segments. The terrestrial segment will be based upon fiber optics and includes the GIG Bandwidth Expansion (BE). Along with GIG-BE, DoD components are developing base and installation-level bandwidth expansion strategies that will provide a bridge from the installation-level telecommunications infrastructure to the expanded GIG. Teleports provide the media junction between space and terrestrial assets. The wireless or radio segment will be based upon the software programmable JTRS. JTRS is a family of software-defined radios with inherent cross-banding and IP routing capability. The space-based segment (Transformational Communication Satellite) will provide satellite communications capability with greatly increased bandwidth and integrated, multi-agency networking capability based on the Internet Protocol.”

[81] Lt Gen Harry D. Raduege, Jr., “Statement for the Record Before The House Armed Services Committee, Terrorism, Unconventional Threats and Capabilities Subcommittee,” available from http://www.defenselink.mil/dodgc/olc/docs/test03-04-03Raduege.doc; Internet; accessed 14 November 2005, 6.

[82] U.S. Department of Defense, “Joint Operations Concepts,” November 2003; available from http://www.netcentricfcb.org/workshop1_references/2_SecDefApprovedJOpsC.doc; Internet; accessed 2 January 2006, 15.

[83] Joint Staff, “Joint C4 Campaign Plan,” 3.

[84] U.S. Department of Defense, “Net-Centric Environment Joint Functional Concept, Version 1.0,” 7 April 2005; available from http://www.dtic.mil/futurejointwarfare/concepts/netcentric_jfc.pdf; Internet; accessed 28 November 2005, 17.

[85] Raduege, 8-9. Lt Gen Raduege specifically stated “Interoperability is the core of jointness. The most reliable strategy for achieving interoperability is the use of a common infrastructure and...services wherever possible. …Weapon systems, sensors, and tactical assets are often highly specialized with C4 capabilities imbedded. Interoperability of these

assets is a prerequisite for the gains in precision and timely integrated operational capability required. Enterprise C4 systems must also achieve this same degree of interoperability." Also note USJFCOM, CRD: GIG, 44, goes on to say "interoperability is the ability of two or more systems, units, or forces to provide services to and accept services from other systems, units or forces to enable them to operate effectively together. This condition is achieved between communication-electronics systems or equipment when information or services can be exchanged directly and satisfactorily between users. The degree of interoperability that can be achieved will be determined primarily by the accomplishment of the IER [information exchange requirements, representing logical interactions and information flows, not physical connectivity]…"

[86] Joint Staff, "Joint C4 Campaign Plan," 41-43. The document elaborates that the goal specifically involves "expanding information sharing…; implementing a communications infrastructure to enable network centric operations – assure seamless, robust, survivable and secure C4 capabilities to the global warfighter; reassess, review and establish policies promoting interoperability and adherence to standards…; identify the requirements to improve DOD/Interagency information sharing; implement GIG NetOps as an end-to-end capability that represents the integrated doctrine, force structure, and TTPs [tactics, techniques, and procedures] needed to manage and direct the network centric operations…; advocate enterprise-wide capabilities and [standardized] tools…[with a] focus…on simplifying network management and security challenges..."

[87] See Joint Staff, "Joint C4 Campaign Plan," 41-46. Several pertinent goals, objectives and action items are presented, including "Goal 1: Transform joint, multinational, and interagency C4 warfighting capabilities to maximize combat effectiveness; Goal 3: Develop highly trained C4 personnel, capable of planning, defending and operating joint, multinational and interagency C4 networks; and Goal 4: Ensure all facets of joint C4 resourcing DOTMLPF [doctrine, organization, training, material, leadership, personnel, and facilities] are synchronized and integrated to maximize Joint Force capabilities." Also, see USJFCOM, CRD: GIG, 36-44, which provides an extensive list of requirements, guiding the heading for NetOps, such as "to accomplish GIG end-to-end situational awareness, systems shall have the NM capability of automatically generating and providing an integrated/correlated presentation of networks and all associated network assets…" and "systems shall have an IDM [information dissemination management, as defined above] capability through which commanders become aware of the information flowing within their AOR to facilitate adjustments to meet operational mission requirements."

[88] Linton Wells, II, Assistant Secretary of Defense (ASD) (Networks and Information Integration [NII])/Department of Defense Chief Information Officer [CIO] (Acting) and LtGen Robert M. Shea, USMC, Director for Command, Control and Communications Systems Directorate [J6], Joint Staff, "Broad NII-J6 Network-Centric Concerns," memorandum for Combatant Commanders, Director, Defense Information Systems Agency, Chief Information Systems Officers, Military Departments, et al, Washington, D.C., 20 May 2005, establishes "we must learn to operate the network as a weapons system…" to better refocus toward network-centric areas.

[89] MG James A. Marks, Commander, U.S. Army Intelligence Center and Fort Huachuca and LTC (P) Steve Peterson, "Six Things Every "2" Must Do—Fundamental Lessons from OIF," *Military Intelligence* , Vol 29, No. 4 (October-December 2003): 11.

[90] See Gentry, 94-95. He asserts "program managers of key systems are not responsible for assuring interoperability with other systems. … While nominally the organizational chief information officers and agency heads have such responsibilities, in practice the acquisition of single systems occurs largely independently. This sometimes leads to what some DOD IT professionals call "drive-by fieldings"—surprise delivery of IT for which users are neither technically nor financially prepared." This shows the pervasiveness of the problem, and need to take a new approach to fix it.

[91] Joint Staff, "Joint C4 Campaign Plan," 25.

[92] Linton Wells, II, Assistant Secretary of Defense (ASD) (Networks and Information Integration [NII])/Department of Defense Chief Information Officer [CIO] (Acting) and LtGen Robert M. Shea, USMC, Director for Command, Control and Communications Systems Directorate [J6], Joint Staff.

[93] USJFCOM, "Joint Transformation Roadmap," 180-181, states "in order to ensure that it is both useful and relevant to future joint operations, however, the GIG should include a time-phased specification of future capabilities linked to current investments, including both the network architecture and associated utilities. Moreover, this specification should include plans and architectures…showing how separate Service network development efforts will contribute to and will be compatible with the broader GIG architecture."

[94] Gentry, 94-99, asserts "the lack of centralized accounting of DoD equipment means that there is not and, given current institutional arrangements, cannot be "enterprise" management of DOD's IT. …the physics of network communications is much less tolerant of incompatible technical designs and inconsistent execution. The fractured design and control of DOD's IT infrastructure creates opportunities for attackers" and "…the services and Defense agencies refuse to obey the spirit and letter of sometimes long-standing policies and continue to buy systems for their use alone" as well as "DOD has failed to comply with the Clinger-Cohen Act of January 1996, which mandates that federal agencies use fairly standard private sector techniques to measure the effectiveness of IT investments. In order to assess the cost-effectiveness of new programs, decision makers must understand the value and effectiveness of the existing assets the new IT will interface with or replace."

[95] Ibid, 99-100.

[96] JP 0-2, III-17.

[97] JP 0-2, x.

[98] USJFCOM, "Joint Transformation Roadmap," 62.

[99] U.S. Department of Defense, "Joint Operations Concepts," November 2003; available from http://www.netcentricfcb.org/workshop1_references/2_SecDefApprovedJOpsC.doc; Internet; accessed 2 January 2006, 6, states "people remain the centerpiece of successful joint operations. Although the capabilities associated with the tools of warfare will change, the dynamics of human interactions and will, instilled through innovative leadership, will remain the driving force in all military operations. Fundamental to the successful utilization of improved capabilities will be the capacity of the individual Soldiers, Sailors, Airmen, Marines and Coast

Guardsmen to learn and adapt to new mission demands, bear the hardships of combat and work diligently to synchronize Service efforts."

[100] Joint Staff, "Joint C4 Campaign Plan," 41.

[101] USJFCOM, "Joint Transformation Roadmap," 62. The Roadmap states "The U.S. Joint Forces Command will…ensure that NetOps activities are an integral part of Joint Exercises and Experiments."

[102] U.S. Chairman of the Joint Chiefs of Staff, *Joint Warfare of the Armed Forces of the United States*, Joint Publication 1 (Washington, D.C.: CJCS, 14 November 2000), I-7.